Report di Laboratorio:
Exploit Java RMI con Metasploit

Analisi Vulnerabilità e Post-Exploitation su Target Metasploitable

Josh Van Edward D. Abanico

23 gennaio 2026

Sommario

Il documento illustra le attività di Penetration Testing condotte sul servizio Java RMI (Remote Method Invocation) esposto dalla macchina target Metasploitable. L'attività si suddivide nella configurazione dello scenario di rete, identificazione del modulo di exploit corretto all'interno del framework Metasploit, esecuzione dell'attacco e successiva raccolta di evidenze tramite sessione Meterpreter, in conformità con i requisiti operativi assegnati.

Indice

1 Obiettivo dell'Esercitazione

L'obiettivo primario è sfruttare una vulnerabilità nota nel servizio **Java RMI Server** in ascolto sulla porta **1099**. Utilizzando il framework **Metasploit**, condurremo un attacco strutturato nelle seguenti fasi:

1. Configurazione e verifica dei parametri di rete (Attaccante e Vittima).
2. Ricerca del modulo di exploit specifico per Java RMI.
3. Configurazione ed esecuzione dell'exploit per ottenere una reverse shell.
4. Post-Exploitation: raccolta informazioni di rete e routing tramite Meterpreter.

2 Fase 1: Configurazione dello Scenario

Prima di avviare l'attacco, è stato necessario configurare le interfacce di rete delle macchine virtuali secondo i requisiti del laboratorio:

- **Attaccante (Kali Linux):** IP assegnato 192.168.11.111.
- **Vittima (Metasploitable):** IP assegnato 192.168.11.112.

Le figure seguenti confermano la corretta applicazione delle configurazioni.

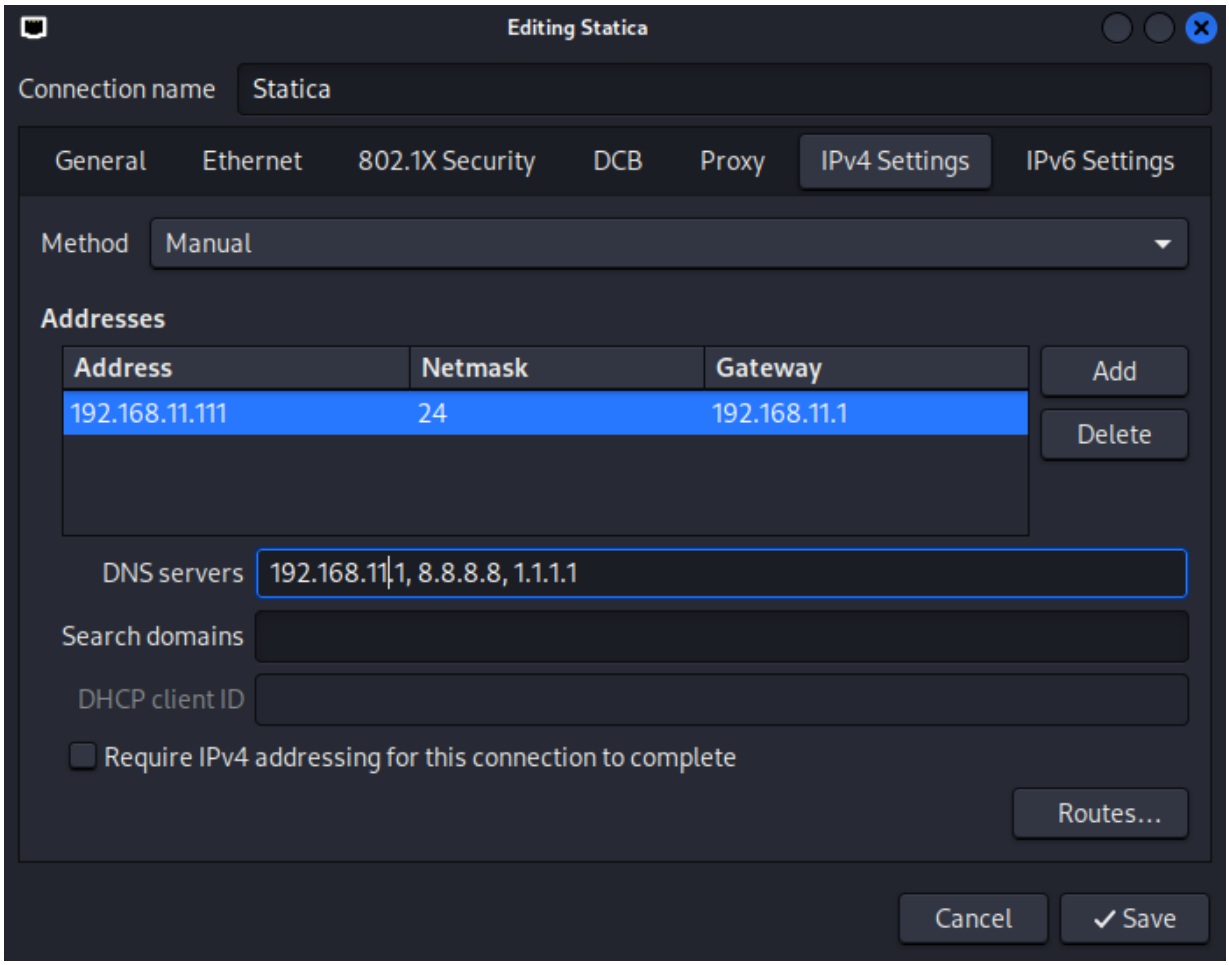

Figura 1: Configurazione IP statico sulla macchina attaccante (Kali).

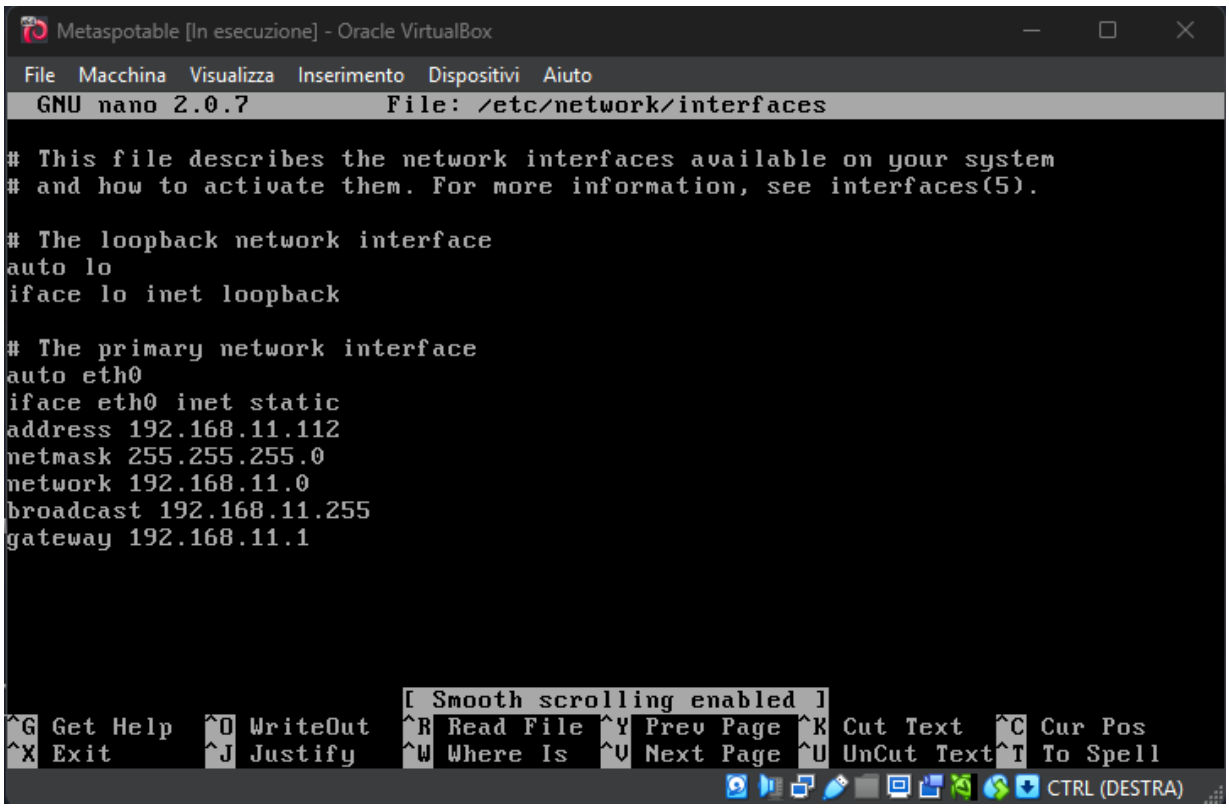

Figura 2: Verifica configurazione IP sulla macchina vittima.

3 Fase 2: Ricerca e Selezione dell'Exploit

Avviato il framework Metasploit, è stata effettuata una ricerca per individuare i moduli relativi a "java rmi". **Comando utilizzato:** `search java rmi`

Dall'output della ricerca, è stato selezionato l'exploit `exploit/multi/misc/java_rmi_server` (indice 8), noto per sfruttare configurazioni insicure predefinite del servizio RMI.

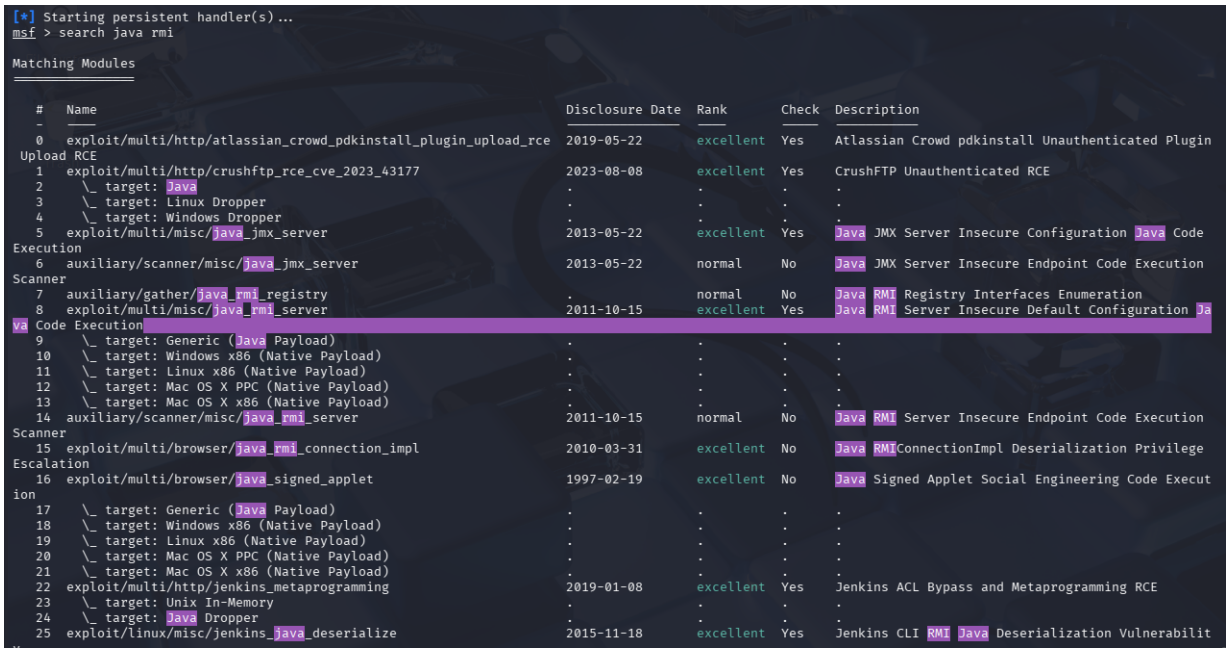

Figura 3: Ricerca dei moduli Java RMI in Metasploit.

4 Fase 3: Esecuzione dell'Attacco

Dopo aver selezionato il modulo, si è proceduto alla configurazione dei parametri essenziali per stabilire la connessione inversa (Reverse TCP).

4.1 Configurazione dei Parametri

Sono stati impostati i seguenti valori tramite il comando `set`:

- **RHOSTS (192.168.11.112)**: L'indirizzo IP della macchina target.
- **LHOST (192.168.11.111)**: L'indirizzo IP della macchina attaccante (Kali) per ricevere la connessione di ritorno.
- **RPORT**: Lasciato al valore di default 1099.

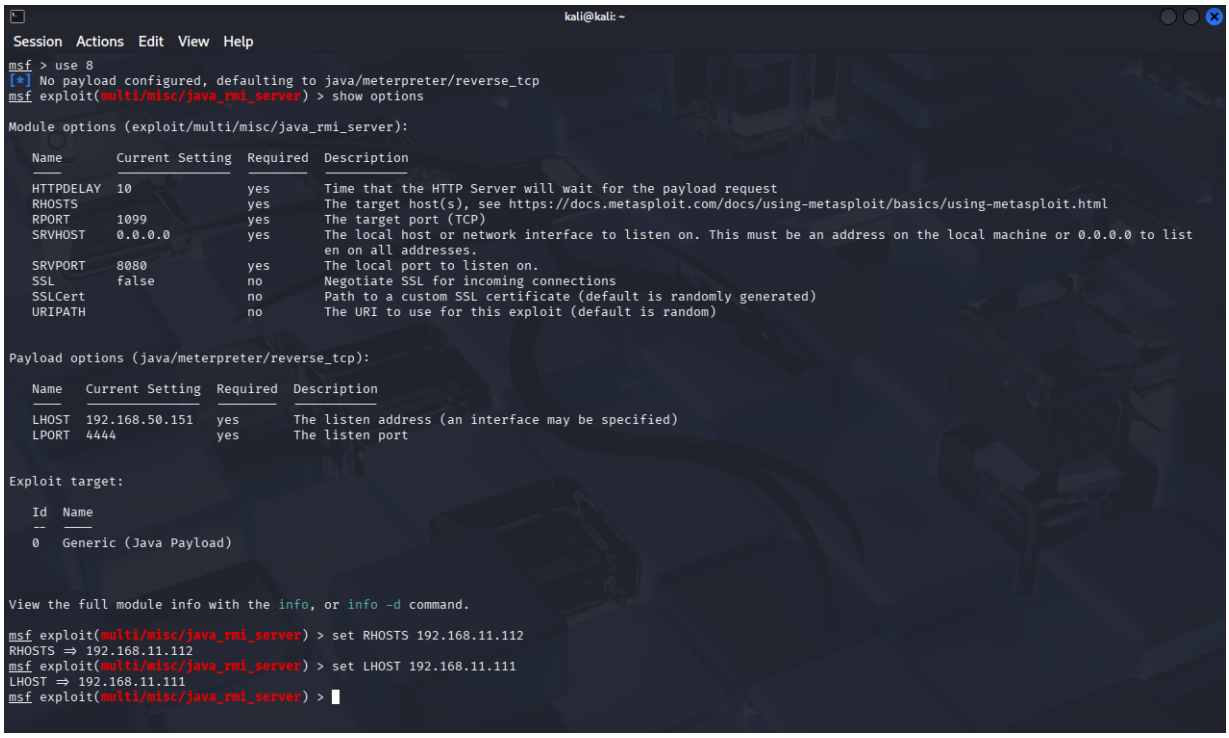

Figura 4: Configurazione delle opzioni RHOSTS e LHOST.

Lanciando il comando `exploit`, il modulo ha inviato correttamente l'RMI Header e il payload JAR. La vulnerabilità è stata sfruttata con successo, aprendo la sessione **Meterpreter 2**.

Figura 5: Esecuzione dell'exploit e apertura della sessione Meterpreter.

5 Fase 4: Raccolta Evidenze (Post-Exploitation)

Una volta ottenuto l'accesso remoto tramite Meterpreter, sono state raccolte le informazioni richieste sulla configurazione di rete della macchina compromessa.

5.1 Configurazione di Rete

Utilizzando il comando `ipconfig` all'interno della sessione Meterpreter, è stata verificata la configurazione delle interfacce di rete della macchina remota.

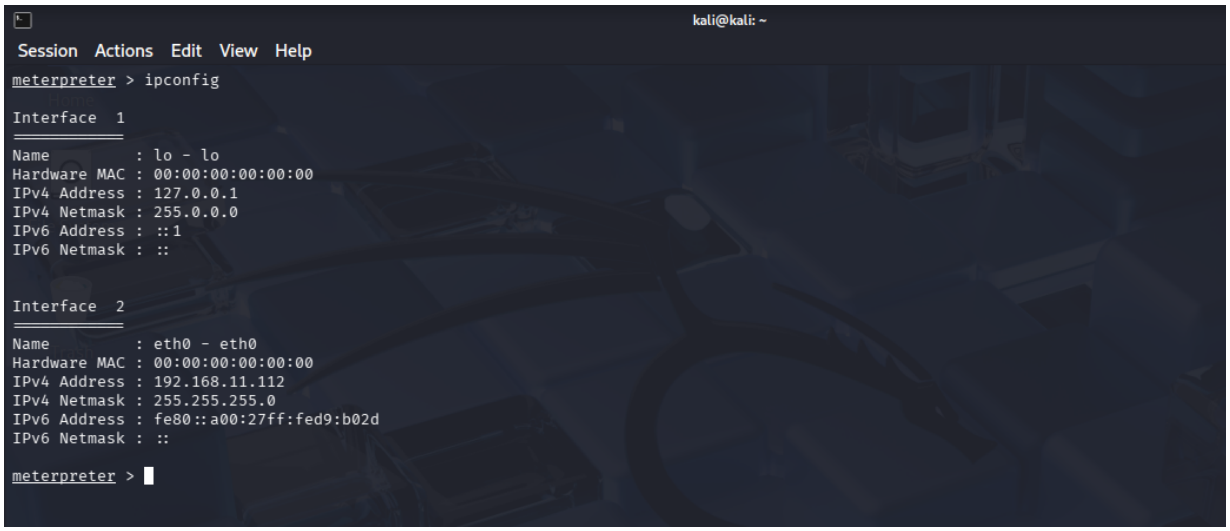

Figura 6: Output del comando ipconfig sulla macchina vittima.

5.2 Tabella di Routing

Successivamente, è stata analizzata la tabella di routing tramite il comando `route`, evidenziando le sottoreti raggiungibili dal target.

Figura 7: Visualizzazione della tabella di routing del target.

6 Conclusioni

L'esercitazione ha dimostrato con successo la criticità del servizio Java RMI quando configurato con impostazioni di default insicure. L'utilizzo del modulo `java_rmi_server` di Metasploit ha permesso di ottenere rapidamente un accesso privilegiato al sistema, bypassando le normali procedure di autenticazione.

L'accesso Meterpreter ottenuto ha garantito il controllo completo per le attività di post-exploitation, permettendo l'enumerazione delle interfacce di rete e delle rotte, come richiesto dalla traccia del laboratorio.